SUPPORT SMALL AND MEDIUM ENTERPRISES ON THE DATA PROTECTION REFORM II

Report on the SME experience of the GDPR

Deliverable **D2.2** (Version 1.0)

Dr David Barnard-Wills, Ms Leanne Cochrane, Mr Kai Matturi, Dr Filippo Marchetti

Budapest – Brussels – Waterford

July 2019

distribution level: **Public**

LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES VRIJE UNIVERSITEIT BRUSSEL

TRILATERAL RESEARCH

Authors	
Name	Partner
David Barnard-Wills	TRI
Leanne Cochrane	TRI
Kai Matturi	TRI
Filippo Marchetti	TRI
Internal Reviewers	
Name	Partner
Lina Jasmontaite	VUB-LSTS
Paul de Hert	VUB-LSTS
Júlia Sziklay	NAIH
David Wright	TRI

Institutional Members of the STAR Consortium		
Member	Role	Website
Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)	Project Coordinator	naih.hu
Trilateral Research Ltd. (TRI)	Partner	trilateralresearch.com
Vrije Universiteit Brussel (VUB) Research Group on Law, Science, Technology and Society (LSTS)	Partner	https://lsts.research.vub.be/

This report has been prepared for the European Commission's Directorate-General for Justice and Consumers (DG JUST).

The STAR II project (Support small and medium enterprises on the data protection reform II; 2018-2020) is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2017) under Grant Agreement No. 814775.

Permanent link: TBC

version 1.0
14 July 2019

Table of Contents

1. Background to the STAR II project

The STAR II project (Support small and medium enterprises on the data protection reform II) commenced in August 2018 and is intended to run for a two-year period. It is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 and is aimed at: (i) assisting European Union (EU) Data Protection Authorities (DPAs) raise awareness about the General Data Protection Regulation (GDPR) among small and medium enterprises (SMEs); and (ii) assisting SMEs to comply with the GDPR.

There are 22 million SMEs in the EU who form the core of the EU enterprise policy. These SMEs face distinctive challenges from data protection law and can often not afford professional legal advice. As such, they merit special support from public authorities as recognised by Recital 132 of the GDPR which specifies that when undertaking awareness-raising activities addressed to the public, data protection authorities should include specific measures directed towards, among others, SMEs.

This report is an analysis of the SME experience of the GDPR during its first year (Deliverable 2.2). The results found within the report, along with the associated report on the review of the state-of-the-art in DPA awareness-raising activities aimed at SMEs (Deliverable 2.1), will serve to inform the tools produced by the STAR II consortium partners to assist both DPAs and SMEs with their respective responsibilities. The STAR II project outputs will include:

1) An email hotline run by the *Nemzeti Adatvédelmi és Információszabadság Hatóság* (NAIH) in both Hungarian and English;
2) A guidance document for DPAs on good practices in awareness-raising techniques among SMEs;
3) A handbook for SMEs to help them comply with the GDPR.

At the time of writing, the NAIH is currently operating the email hotline and has completed an awareness-raising campaign in Hungary to promote the hotline among SMEs. An analysis of this effort along with Deliverables 2.1 and 2.2. and the validation workshops will ensure that the guidance document for DPAs and the handbook for SMEs is innovative and responsive to the core aim of assisting SMEs comply with their GDPR obligations.

1.1. STAR projects, 2017-2019

The STAR II project follows on from the STAR project (Support training activities on the data protection reform), which is nearing completion and focused on providing support to the

training activities of DPAs and data protection officers (DPOs) on the EU data protection reform, especially the GDPR. The STAR project was also co-funded by the EU under the Rights, Equality and Citizenship Programme 2014-2020. The outputs from the STAR project have included:

1) Training scenarios for each training category,
2) A Seminars' Topics List, based on the training scenarios,
3) Seminar Material for each one of the seminars,
4) Webinars (selected from the Seminars' Topics List),
5) A training Handbook,
6) A takeaway reference GDPR checklist,
7) A ten-point GDPR introductory list.

2. Executive summary

This report presents the findings from a multi-method research study into the experiences of small and medium enterprises (SMEs) with the General Data Protection Regulation (GDPR). The project team conducted interviews with SME associations, an online survey of EU SMEs and face-to-face interviews with SMEs. The intent of the study was to understand what SMEs had done and were doing in relation to the GDPR, where they were getting information and support, what challenges they were facing, and what actions from data protection authorities and others would be helpful for them. Our top-line findings include:

- SMEs may be aware of the GDPR, but they're lacking resources to get them to adequate level of compliance. "awareness" might be less of a problem than "capacity".
- Very high demand for templates and practical guides
- Many SMEs think that the GDPR is done and settled.
- A minority of SMEs feel it is now too late for DPAs to produce guidance, but the majority would still be receptive to new guidance, if clear, specific and practical.
- There is a high level of scepticism about GDPR experts and consultants.
- SME associations are playing an important role in supporting those SMEs that are members.
- Data protection challenges for SMEs are quite diverse, however common challenges include:
    - Understanding what changes need to be made to be compliant
    - Designing and developing new processes and procedures concerning personal data processing
    - Getting staff to understand the importance of data protection
- SMEs want guidance on technical and organisational measures for (personal) data protection
- There are some SMEs whose data protection could be improved by making them aware that there is basic guidance available. However, many others have quite specific questions and concerns.
- SMEs find it challenging to assess proportionality and data protection risks of their operations and would rather have clear steps to take to comply with requirements stemming from the GDPR.
- SMEs that consider themselves very familiar with the requirements of the GDPR are different to other SMES:
    - More likely to contact DPA as well as to access DPA guidance. Such SMEs tend to find that guidance more useful that SMEs not acquainted with the GDPR.

- DPAs need to be careful not to cater solely to this category of SMEs, who they are mostly likely to encounter.

3. List of Abbreviations

DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ePrivacy Directive	Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ELI: data.europa.eu/eli/dir/2002/58/oj)
EU	European Union
GDPR	General Data Protection Regulation (Regulation EU 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, ELI: data.europa.eu/eli/reg/2016/679/oj
SME	Small and medium enterprise
STAR	Support training activities on the data protection reform
STAR II	Support small and medium enterprises on the data protection reform II
WP29	Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46/EC (Article 29 Working Party). WP29 was replaced by the EDPB on 25 May 2018. The EDPB has endorsed many WP29 GDPR-related guidelines.

4. Introduction

This report is the second public report of the STAR II project.[1] This report attempts to map the recent experiences of small and medium sized enterprises (SMEs) within the EU, on the basis of interviews with SME associations, industry and sectoral bodies, an online survey of EU SMEs, and a series of face-to-face interviews with SMEs. This report is published in conjunction with a study on the activities and perspectives of EU data protection authorities (DPAs) in relation to guidance provided for SMEs[2]. The two reports share a set of recommendations which are available in each document.

The European Union has recently been through a lengthy process of data protection reform. One of the most significant components of this was the General Data Protection Regulation (GDPR). Formally, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data, and repealing Directive 95/64/EC (General Data Protection Regulation), but most often shorted to "the GDPR". It was adopted in 2016 and came into effect in May 2018. The objective for the data protection reform was to achieve a high and uniform level of protection of personal data in the EU, protecting people's personal data, whilst at the same still allowing for the development of technological services and innovation and of a digital single market.

The law contained several novel elements, particularly data protection by design (Art 25) and data protection impact assessment (DPIA, Art 35).

Small and Medium Enterprises (SMEs) are defined as any enterprise which employs fewer than 250 persons, and which have an annual turnover not exceeding €50 million. 9 out of every 10 enterprises in the EU is an SME and they are understood to generate two out of every three jobs. Given this, it is a policy objective of the European Commission to promote entrepreneurship and improve the business environment for SMEs.[3]SMEs are explicitly mentioned in the text of the GDPR – Recital 13 indicates that one motivation for the Regulation was to provide "legal certainty and transparency for economic operators, including micro, smalls and medium sized enterprise". Article 132 states that "Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized

[1] Disclaimer: The content of this report represents the views of the authors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
[2] STAR II project, Deliverable D2.1
[3] European Commission, User guide to the SME Definition, Luxembourg, 2015, https://ec.europa.eu/regional_policy/sources/conferences/state-aid/sme/smedefinitionguide_en.pdf

enterprises". The regulation also provides some specific exemptions to SMEs – for example, reduced requirements around records of processing activities for non-regular processing (Article 30). However, commentators have expressed concern about the level of GDPR knowledge and awareness amongst European SMES.[4]Furthermore, the European Commission had observed the vulnerability of SMEs regarding the GDPR. It stated in its press release, inter alia, that "[t]here is in particular a need to step up awareness and accompany compliance efforts for SMEs"[5].

In this context The STAR II project aims to tackle lack of awareness by creating several awareness-raising tools and campaigns targeting SMEs throughout Europe and overseas. This final objective will be achieved by:

- Reviewing the state of the art in Data Protection Authorities' (DPAs) awareness-raising activities, including conducting stakeholder engagement activities to hear their points of view and planning effective, subsequent activities (STAR II D2.1)
- **Reaching out to SMEs to analyse their experience with the GDPR in the first months of its applicability (this report).**
- Running awareness-raising campaigns to ensure that the widest possible number of companies knows about their obligations under the GDPR regime
- Assist SMEs by setting up a trial hotline to respond to SMEs' questions and doubts
- Assist DPAs by creating a digital guide containing information on the best practices in running a hotline and running awareness-raising campaigns.
- Providing a solid base for GDPR implementation by creating an innovative, FAQ-based handbook for SMEs on EU personal data protection law

This report contains the results from the second activity. The next chapter sets out our research methodologies, before subsequent chapters explore GDPR knowledge and awareness regarding the GDPR; Key challenges for SMEs; how data protection authorities might be able to assist SMEs; and insights from the study for the next steps in the STAR II project. The conclusions to the report are shared with the partner report D2.1.

[4] Ashford Warwick, "Most UK small businesses in the dark over GDPR", ComputerWeekly.com, 07.11.2017; http://www.computerweekly.com/news/450429625/Most-UK-small-businesses-in-the-dark-over-GDPR.

[5] On the role of DPAs, cf. e.g. Colin Bennett & Charles Raab, The governance of privacy: policy instruments in global perspective, Ashgate Publishing, 2003.

5. Research methodologies

We used a combination of three research methods to help us find out about SMEs experiences with the GDPR. Firstly, we conducted a series of interviews with representatives of SME associations. Second, we ran an online survey addressed to SMEs themselves, and third, we supplemented this survey with face to face interviews with SMEs.

5.1. Interviews with SME associations

The STAR II consortium was able to conduct interviews with representatives of **22** different associations which include SMEs in their membership. These included associations in UK (x2), Latvia, Greece, Belgium (x2), Malta, Cyprus, Denmark (x3), Ireland (x2), and Spain, as well as with five Europe-wide associations, one global and one based in Latin America. These interviews asked similar questions to those we gave to SMEs themselves in the survey and interview research. The aim with the SME association interviews was to get the associations perspective on their members priorities, experiences and concerns but also to supplement this perspective with that of organisations that had time to give attention to GDPR issues. Europe-wide associations sometimes took the form of umbrella organisations with national level associations forming part of their membership. Such organisations tended to focus on the trans-national concerns for SMEs and European infrastructure and policy framework; whereas national associations conveyed more detail on the day to day concerns of SMEs.

5.1.1. How do associations know about the GDPR concerns of their members?

We asked the association representatives what their knowledge was about the GDPR issues their members (and the SME sector more broadly) were experiencing. This was an important first step for understanding how to interpret the information they provided. The biggest consistent source of knowledge of the SME associations we spoke with was the ongoing day-to-day contact with their membership, through events, helplines and other fora. In addition to this, several associations had conducted specific research into the GDPR issues facing their members while others were planning to do so in the future. Only a small number of the associations we spoke with said they had done no research into members experience of the GDPR. However, given we identified and contacted a broader sample of 96 organisations, we might assume that the organisations who responded to the study were those that were more active or aware in this field.

The organisations we spoke with were active in the data protection space and had a range of channels for gathering information. The ways in which SME associations find out about

their members experience of the GDPR included: memberships surveys, board level discussions, participation in national consultation processes with relevant government ministries, cooperation with other stakeholders; unofficial/informal liaison approaches (talking with members on ongoing basis); participation in third party events and conferences; running regional tours/roadshows and seminars/conferences; providing a GDPR hotline for members; assigning specific staff to GDPR-related issues; focused surveys on the costs associated with GDPR compliance; accessing studies conducted by individual members of the associations and finally, consumer privacy perception surveys. The above range of research methodologies reflects the specific needs and strategic direction of the various membership bodies but it also means that the knowledge base on SME experiences is currently far from comparable across sectors and across EU member states.

5.2. SME Online survey

We ran the survey between December 2018 and June 2019. In total, we had 119 visits to the survey with a survey completion from approximately **52-60** respondents (with some variation on how many skipped each individual question).

Our survey data does not, unfortunately, cover all the EU Member States. The survey had the highest number of respondents in Denmark (34), Hungary (29), and the United Kingdom (11), with the remainder of the respondents operating SMEs in Germany (2), Ireland (2), Croatia (1), Finland (1), Malta (1), Netherlands (1), Slovenia (1), and Spain (1). The likely reasons for this bias are the operating languages of two of the partners (TRI IE and NAIH) and the active distribution of the survey by a Danish SME association. The potential impacts of this distribution are that care should be taken when generalising from this data to all European SMEs. As a result, this analysis is explorative and should be used to generate ideas, (for example lists of challenges that SMEs are facing) but is less strong for ranking or quantifying.

Our sample also displays some bias towards SMEs involved in technology – this is not typically representative of the SME sector but is indicative of those SMEs that are likely to be engaged in the processing of personal data in non-routine or significant manners, and particularly involved with digital data. This is likely a result of respondent bias – SMEs interested or thinking about the GDPR may be more likely to respond to a survey request about the GDPR. However, the data also includes a spread across the common SME sectors. For example, responses received for the “other” category included: business consultant, market research, non-profit/NGO, arts, rental, security, marketing, accounting and recruitment.

5.3. Face-to-face Interviews with SMEs

STAR conducted **eleven** face-to-face interviews with SMEs. The purpose of these face-to-face interviews allowed us to check the representativeness of the online survey and be more confident in its findings. The interviews were conducted with SMEs set up in the UK (Northern Ireland and England), France, Greece, Ireland and Poland.

The face-to-face interviews allow us to assess the potential bias in the online survey. We know that our face-to-face interviews have a profile closer to that of the SME sector in general, including companies in media, healthcare, transport and logistics, tax advice, midwifery, pharmacy, childcare, retail, beauty and viticulture, and a higher proportion of organisations where GDPR knowledge is lower. Where the answers from the interviews correlate with those from the survey, we can be more confident about the survey results being generalisable and avoiding sampling bias. For example, if both online and offline respondents are raising the same problems and expressing the same desires for guidance, then we can be more confident that these problems and desires are not just an artefact of our sampling method.

6. SME GDPR knowledge and awareness

From the STAR II research approaches we can build a picture of the baseline level of GDPR awareness amongst EU SMEs, including a sense of where they get information from, how satisfied they are with this information, where they look when they have problems, and the role of both data protection supervisory authorities and other bodies and organisations in this landscape.

6.1. Current level of GDPR awareness of SMEs

The associations assessed the level of GDPR awareness amongst their members in variable ways, both within and among their various memberships (depending on the nature of the association e.g. sector specific, country specific or wider umbrella organisation).

A small group assessed their members awareness of GDPR issues as high – in that there was high awareness that there are new rules, and that there is a need to comply, and that their supporting materials and guidance or communications on the topic of GDPR are amongst their most accessed. The high level of attention to the GDPR in the news over the past year had reached their members, with one national association stating that a high-profile case against an SME, with resulting caselaw, had created a high level of awareness amongst their membership. This group drew attention to the role of their own awareness raising efforts in this high level of awareness.

Other associations felt that their memberships awareness of the GDPR was either moderate or variegated -their members were "making efforts to be compliant" but with a big divide between smaller and larger enterprises. They identified higher levels of awareness among those members actively engaging with an association's GDPR specialist but also expressed awareness that other SMEs in the sector are doing little or nothing.

Several associations informed us that there was baseline awareness about the GDPR – e.g. they felt that their members knew that it existed, and what it was about, but that awareness of detail was lacking and that this translated into a lack of action. Awareness is there, but implementation is not (e.g. 50% of one industry not in compliance). In particular, awareness of where liability and accountability reside was seen as low.

Several associations felt that SME awareness of the GDPR in their sector or among their membership was poor. Reasons they gave for this low level of awareness included: the complicated nature of the GDPR – being seen as too complicated for SMEs, who might instead "close their eyes to it and hope for the best"; the GDPR being seen as a settled and

done thing, that the job is almost over; or that fines and breaches are only matters of concern for large entities. The latter reason was based on a perception that either small organisations were too insignificant to capture the attention of DPAs or the belief that DPAs did not have the time or resources to investigate them - an absence of fines for SMEs was seen as encouraging this. Some associations expressed that attention on the GDPR may be reducing after the high point of May last year.

Associations also told us that some sectors were "aware" of the GDPR in concept, but not in practice. They also suggested that their members were now highly sceptical about personal data protection compliance related issues. This is mostly because they had been overwhelmed with, for example, adverts for DPOs or compliance services and were now cynical about any material or communications in this domain. Other reasons included the variable quality of services and the receipt of contradictory information.

We asked survey respondents how familiar they felt they were with the requirements of the GDPR. Respondents overwhelmingly selected the options ranging from 'somewhat familiar' to 'extremely familiar' (see Figure 1).

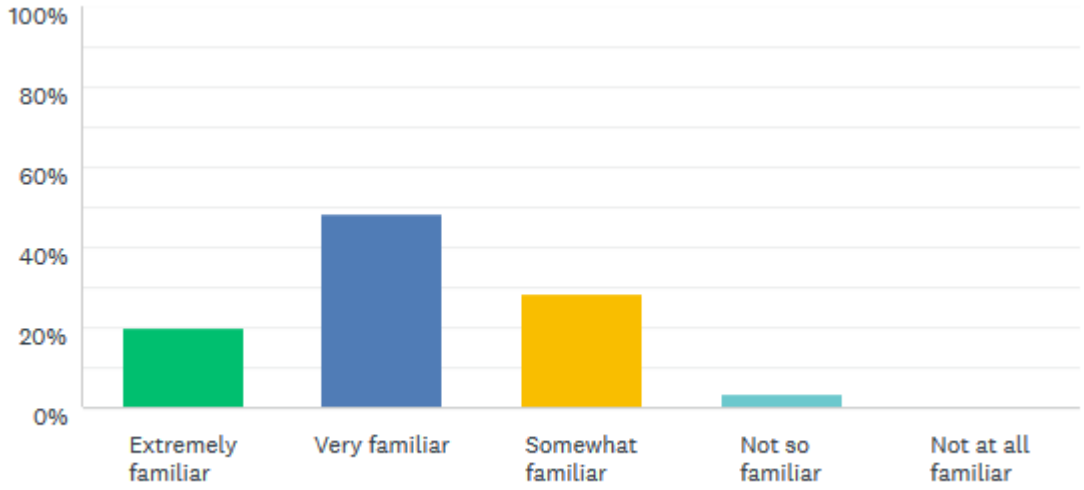

Figure 1: SME Familiarity with GDPR requirements

Whist this looks positive, we should remember self-selection bias and the potential for over-confidence in self-assessment. In our face to face interviews several more SME told us that they did not know anything about the data protection principles in the GDPR, meaning that the likely picture across the SME sector is as mixed as that presented by the SME associations. These self-assessments are however, a useful way of segmenting the responses to other questions asked in the survey.

Several insights on SME GDPR awareness emerged from these interviews:

- SME GDPR awareness is **highly variable** across sectors and Member States.
- DPA activity was seen as a driver of higher awareness, especially in relation to cases, fines and resulting caselaw, as well as creating or endorsing codes of practice.
- Awareness doesn't always lead to compliance or implementation – awareness is often seen as a necessary first step towards GDPR compliance, but often insufficient in the absence of other drivers and influences and the knowledge to put compliance into practice. Many associations told us that awareness was **not the main barrier their members were facing to GDPR compliance**.
    - Organisations being aware and motivated to comply still does not necessarily result in compliance – one of the interviewed organisations suggested that their members sometimes focus on some elements at the expense of others – for example, they become very focused upon the privacy policy on their website, but do not make efforts to understand and examine the data they are processing.
- Poor data protection communication, such as being overly legalistic, can have a negative impact.
- Membership organisations believe that their members are (on average) better informed about GDPR and related issues than non-members.
- Members only want to think about GDPR when they are directly impacted.
- SME awareness depends largely on guidance provided in the language of their jurisdiction:
    - SMEs are likely not aware of guidance from the EDPS or other non-national data protection bodies (e.g., WP29 or the EDPB).

6.1.1. A Typical SME?

We did not ask SME associations generally to outline a typical SME in their context but in the course of conversation one association offered the following comment on the SME sector:

> *"A typical company is one that covers about 60% of scenarios. It looks like this: It is very small, and not very IT literate. Typically, it uses Outlook, PowerPoint and Excel for all its paperwork. It does not process sensitive data, but it has some data including employee data, such as social security numbers, etc".*

6.2. How did SMEs prepare for the GDPR?

The associations told us that many of their members had sought external support from auditors or consultants to become ready for the GDPR. However, several highlighted the high fees charged for such services, whilst others were critical of the quality and appropriateness of GDPR "experts". They contrasted this with the support available from the associations themselves, particularly when this is included in the association's membership fee. Some associations reported a membership spike in April/May 2018, which they associate with the GDPR preparation support they made available to members. Several associations reported that some of their members has sought support for compliance from software companies.

Amongst the SMEs we interviewed directly, about half reported having taken no action to prepare for the GDPR. The other half took a variety of actions including, completing an audit, identifying data they hold, making data protection agreements with partners, updated computer software, introducing cyber security and physical access controls, and outsourcing data protection services.

6.3. Where do SMEs go when they have GDPR questions?

We asked the associations we interviewed "what do their members do when they have data protection questions?" The vast majority suggested that SMEs would look for some form of external expertise. Very few associations expressed an assumption that their members would have a DPO, and several expressed that it was very rare to find an SME with an internally comprehensive understanding of the GDPR. Common answers included asking law firms, data protection professionals and experts (e.g. consultants), asking auditing firms with which they have existing relationships, asking the membership association for support, asking other sectoral associations or bodies (e.g. chamber of commerce), directly asking the supervisory authority, engaging an external generalist law firm, and doing their own research online – searching for ready to use material (but that did not simply repeat "legalese" found elsewhere). The associations commented on the relative accessibility and openness of the national supervisory authority as an important consideration for their members when asking for help, as well as the importance of existing established relationships between SMEs and potential sources of expertise, e.g. with their accountant. One interviewee remarked that they had been asked by the national supervisory authority to prepare a set of questions from the sector, in order to assist with managing the burden upon the DPA of a large volume of individual questions. It was also suggested that larger SMEs are more likely to have access to legal assistance. In terms of the volume of queries coming into SME associations themselves, this was variable, with some reporting a high

number of GDPR-related questions, with others reporting very few. Scepticism of GDPR consultancy was also raised in the context of this discussion.

We asked survey respondents "have you ever used any other [excluding DPAs] sources of data protection and GDPR related guidance. If so, can you tell us these sources?". About two thirds of respondents had sought guidance from somewhere other than their national DPA. Those most commonly reported alternate sources were trade or sectoral associations. In decreasing order, these alternative sources of information were:

- Trade or sectoral associations
- Chambers of commerce / EU bodies (Article 29 working party guidance, the European Commission or the EDPB)[6] / a general online search
- Conference and seminars / Foreign data protection authorities' websites[7]
- Training providers / Law firms / Auditors / IAPP
- Peers and networks / books/ Peer reviewed journals /
- National government

Similarly, the face-to-face interviewees reported accessing guidance from private legal counsel, chambers of commerce and an IT software consultancy. A small number of our interviewees mentioned that they had received lots of commercial proposals for data protection guidance and support. One rejected these sources because they felt that the commercial practitioners that approached them lacked experience.

The high prominence of trade or sectoral associations (including SME associations) supports the general findings that trade or sectoral associations are a significant potential channel for getting data protection guidance to SMEs.

6.3.1. SME awareness and engagement with DPAs

In the survey, we asked "Have you ever seen an advert of awareness campaign from your national data protection authority?" Almost 60% of survey respondents that answered this question said that they had.

[6] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

[7] ICO's website and guidance material were mentioned several times.

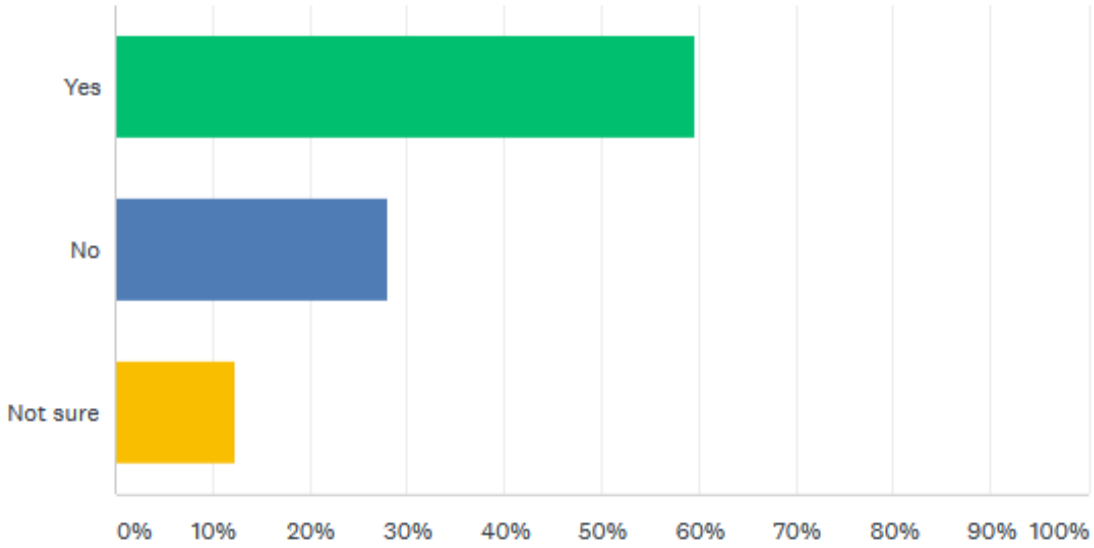

Figure 2: Has the SME seen an advert or awareness campaign from their national DPA?

However, the SMEs that we spoke to in face to face surveys reported a low awareness concerning the functions of their national DPAs.

> *"I know about [DPA] from the news, but I do not really see in what way what they do has anything to do with my business".*

Interestingly in our survey, 57% of our respondents said they had contacted their national DPA. This contrasts strongly with our face to face interviews, where only 1 out of 10 (10%) had attempted to contact their DPA. Our survey data therefore likely over-represents SMEs that contact their DPA.

Using the survey responses, if we contrast the self-reported familiarity of the SME with the GDPR against the question "have you ever contacted your national DPA", we can see that SMEs that consider themselves either extremely familiar or very familiar with the GDPR requirements, are more likely to have contacted the DPA with a query, than those SMEs that consider themselves to be not so familiar or somewhat familiar (see Figure 3). It is likely that knowing something about the GDPR includes 1) knowing that it may be possible to contact the national DPA for advice, and/or 2) includes awareness of GDPR issues that may need an answer from a DPA. SMEs at the start of their GDPR journey may simply not know that they can contact their DPA, whereas more mature companies will come to know that the DPA is a potential source of advice and guidance.

We then asked survey respondents who had contacted their DPA how satisfied they were with the response they received. Positively, the majority were satisfied or very satisfied with the DPA's response (see Figure 4).

We provided an opportunity for respondents who were very dissatisfied to provide a reason for this. Reasons received were:

> *"No concrete guidance given. Their answer basically served to protection themselves from any later complaint".*
> *"The answer was not useful"*
> *"No real answer, not technical support to comply"*
> *"They have not even answered"*
> *"No real response. They are waiting for court decisions"*

In terms of the modes of communication between SMEs and DPAs, the survey asked respondents who had contacted their DPA, how they had done so. The majority used email, followed by those who used the phone. There was a smaller number who had used an online chat function and one who had sent a letter or fax (see Figure 5).

We also considered if there were modes of communication with the DPA that are associated with greater satisfaction amongst the SMEs interviewed. The numbers in this sub-sample are very small, but there's an indication that mode of communication could make some difference to satisfaction. In general, more of the respondents were satisfied or very satisfied with the DPA response than were dissatisfied or very dissatisfied. Email communication is the one mode where there are any very satisfied respondents. The one SME who attempted to send a letter or fax was very dissatisfied with their response. Generally, email and phone appear to have the highest levels of satisfaction amongst SMEs (see Figure 6).This does align with the expressed preferences for SMEs in relation to hotlines and help-desks (see section 9.1)

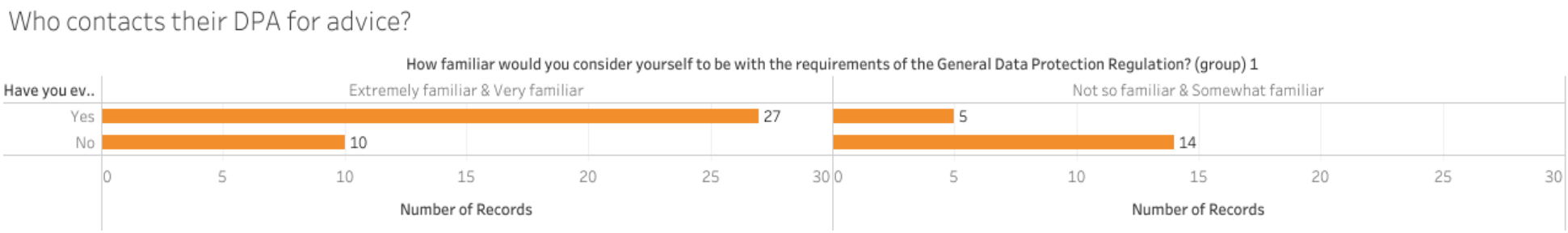

Figure 3: Familiarity with GDPR against contacting DPA

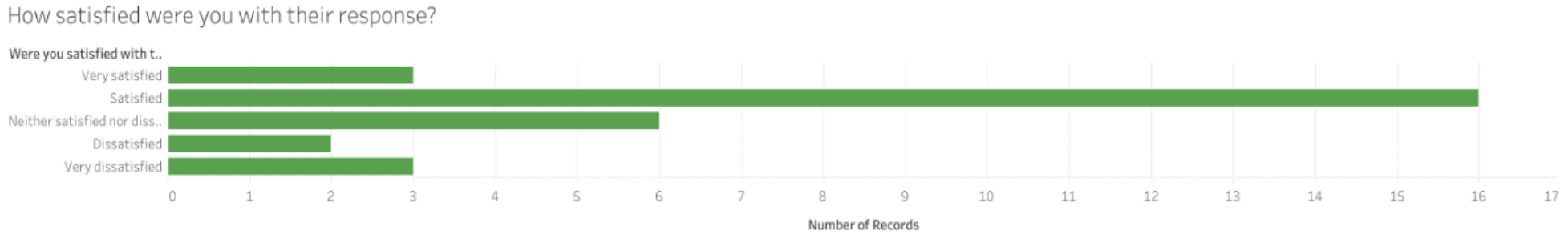

Figure 4: SME satisfaction with DPA response to contact

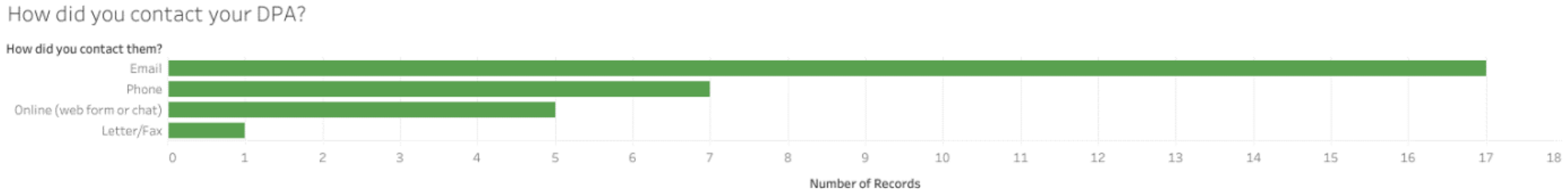

Figure 5: How did SMEs contact their DPA

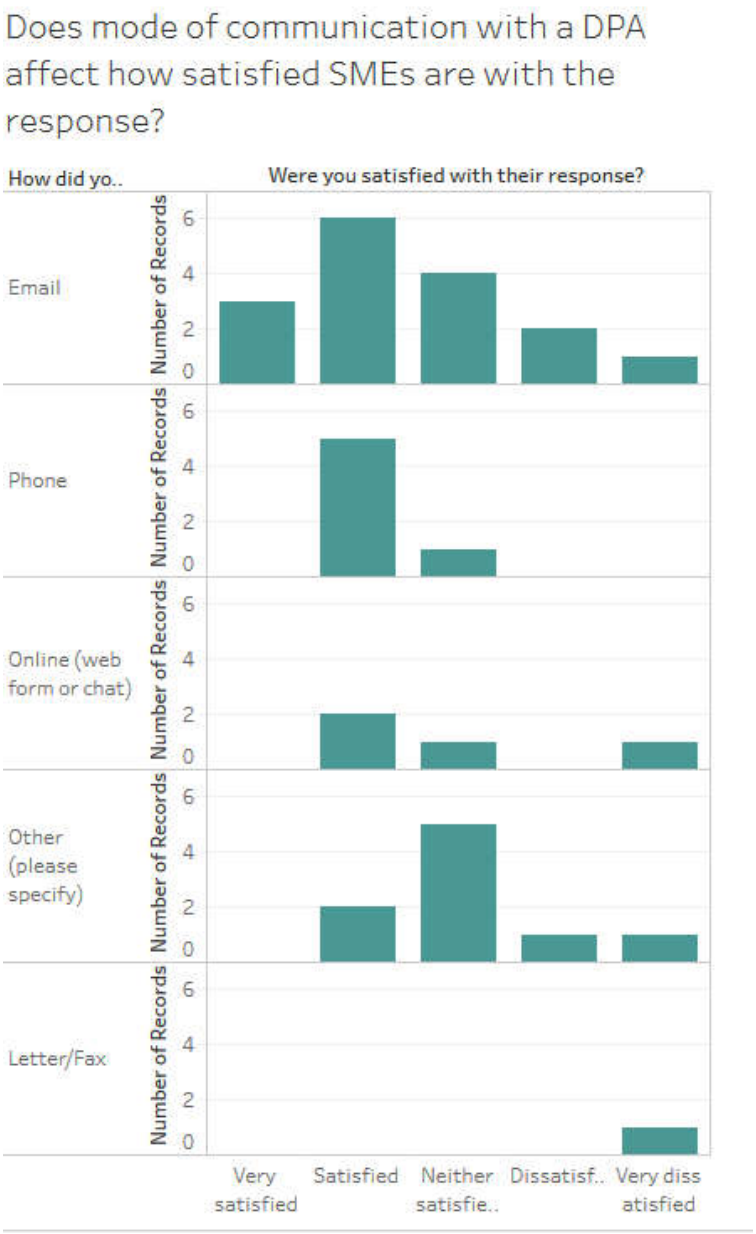

Figure 6: Mode of communication with DPA against response satisfaction

Before turning to the issue of DPA guidance (which associations deemed to be of good quality, and were willing to recommend it to their members), it is of note that SME associations expressed that they did not feel that SMEs in general were aware of such resources (see section 6.3.). It was suggested that profit-making data protection advisors might be unwilling to promote the free tools and resources that are already in existence. There was also little awareness of active advertising or promotion by DPAs of their *guidance* materials (in spite of the findings in Figures 2 and 3) and evidence that finding DPA guidance material required a proactive checking for information and resources by the SMEs.

6.4. Guidance from DPAs

In the survey, we asked "In the last six months, how often have you accessed any guidance from your national data protection authority?" Whilst about a fifth of respondents had not accessed DPA guidance in this period (which meant that just under 80% had accessed DPA guidance at least once), there was also a small group of SMEs who were accessing guidance from their DPA on a very regular basis (i.e. more than 10 times in last six months).

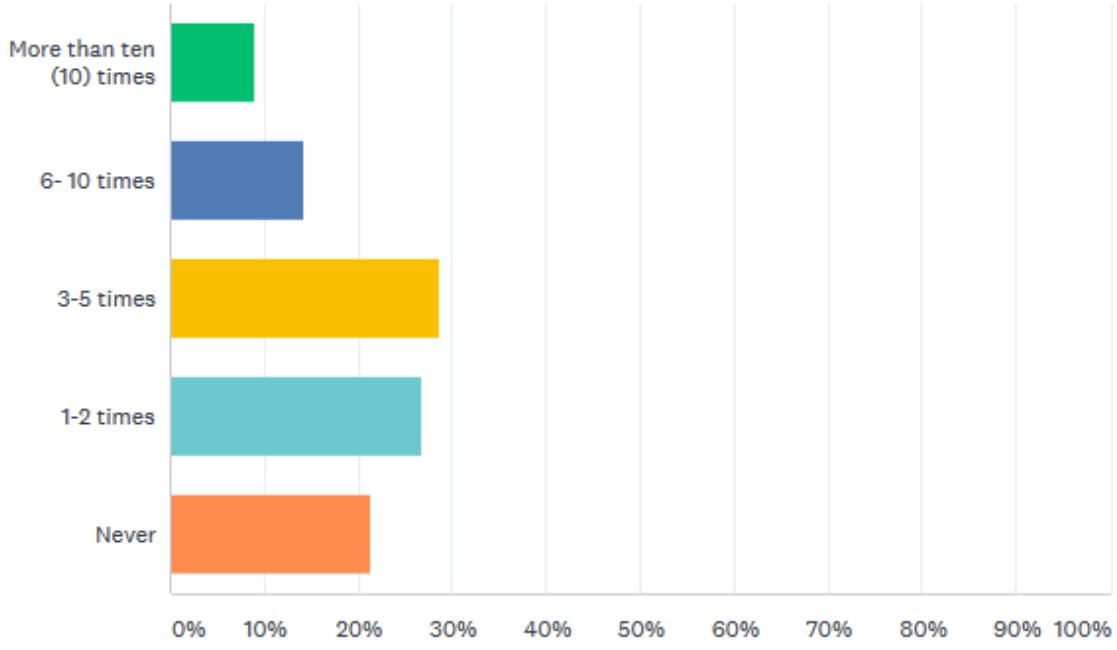

Figure 7: SME access of DPA guidance in the last 6 months

The respondents were then asked how useful they had found this guidance.

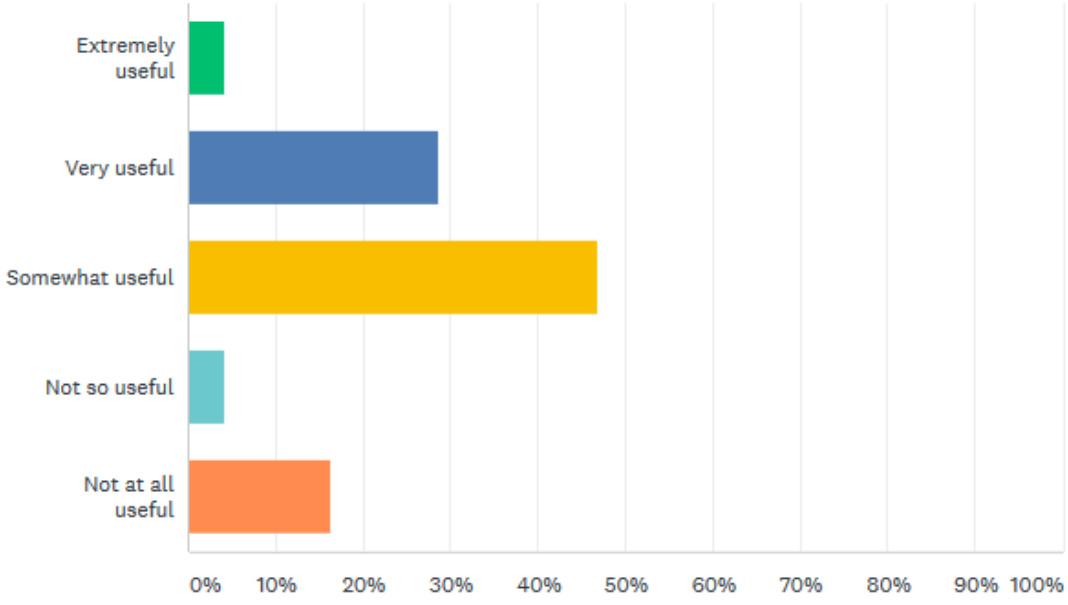

Figure 8: how useful have SMEs found DPA guidance

With SME associations, we also discussed the adequacy of guidance provided by the DPAs. Generally, the belief was that the DPAs were doing an adequate job of producing guidance, highlighting key issues, providing information on their website and answering queries. Several respondents suggested that there had been some limitations, e.g. missing guidance in the run-up to the GDPR coming into force and in months afterwards. At the same time, the respondents said they felt the situation was improving.

The interviews identified several factors that had undermined SME associations confidence in the GDPR guidance coming from supervisory authorities. If not suitable for SMEs then associations may have concerns about recommending them to their members. This list is an aggregate of issues identified but taken together are the **risk factors for a loss of confidence** (see box below).

6.4.1. What makes SMEs lose confidence in DPA guidance?

What makes SMEs lose confidence in the DPA Guidance?

- Overly generic guidance – the organisation must infer from it and make assumptions about how it should be interpreted in their specific situation.
    - Guidance raises more questions than it answers
- Difficulty in reaching a DPA with specific questions and getting concrete answers.
    - Feeling that the DPA is overloaded – particularly at time of GDPR coming into force
    - Taking a long time to get a question answered – e.g. having to spend a long time waiting on a phone, long wait times for email queries.
    - Knowledge level of the DPA staff responding to queries tends to vary
    - No EDPB helpdesk (for cross-EU traders)
    - Not getting an answer to a question
- Limited DPA guidance (due to structural issues with the DPA)
- Conflicting guidance (either internally contradictory or a national DPA contradicting guidance from the EPBD, for example).
- Too academic / legal theory to be useful for everyday use, particularly for SMEs. Not user-friendly. Described by one interviewee as "The rules and guidance are designed for much bigger companies, where there is one or two specialist people just dealing with the issue. They are not for people doing paperwork late at night at the kitchen table after being in the field all day"
    - Perception that DPA only engages with larger data controllers, not with SMEs.
- Guidance arriving too late – GDPR guidance was seen by several associations as particularly time-sensitive. Whilst their members do need to comply, they perceived a window for changing behaviours and practices that may have passed.
    - Organisations had to make decisions without up-to-date guidance
    - Old information/rules on website for too long – 95/45/EC rules into the GDPR period.

Conversely, what seems to increase confidence in the guidance available, includes communication and collaboration with the associations – for example, one SME association appeared to express some investment in the DPA guidance on the basis that they had been shown it in advance providing an opportunity for some input. Open-access, free-to-use materials from DPAs were appreciated, as was DPA attendance at industry events.

Several interviewees remarked that whilst they evaluated the guidance available from DPAs to be good quality, and were willing to recommend it to their members, they did not feel that SMEs in general were aware of these resources (see also section 6.2.1.).

We can get more insight on this issue by breaking down the usefulness of DPA guidance by how familiar the SME respondent considers themselves to be with the requirements of the GDPR (see Figure 9a). This provides some very indicative suggestions about who might be well served by DPA guidance. Ideally, each level of familiarity would consider DPA guidance to be very or extremely useful. Across the whole sample, most respondents think it is somewhat useful (23).

Those who consider themselves extremely familiar are spread in their assessment of the usefulness of DPA guidance they have accessed. They are the only category to consider DPA guidance extremely useful (and this is only two respondents). Those who consider themselves very familiar largely think DPA guidance is either somewhat useful or very useful. This could suggest that those familiar with the GDPR, are having their guidance needs broadly met by the DPAs. The somewhat familiar and the not so familiar are perhaps less well served by existing DPA guidance, than the extremely and very familiar (who are more likely to think that DPA guidance they have accessed is somewhat useful or better) (Figure 9b).

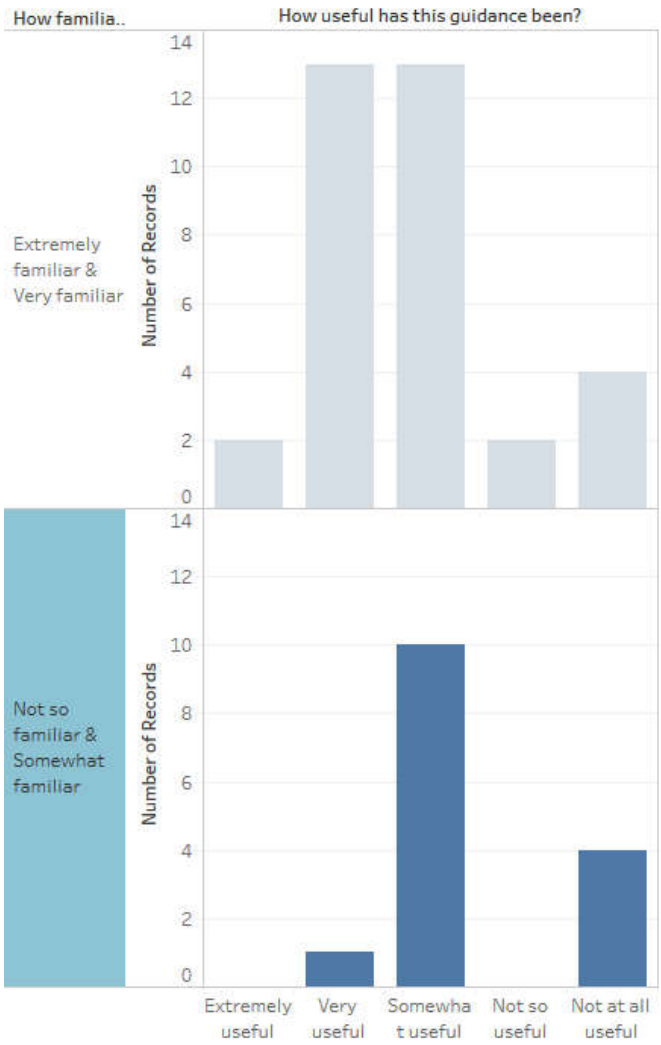

Figure 6b: Grouped chart on familiarity with the GDPR against usefulness of available guidance

Finally, some respondents suggested that there was a desire among some SMEs for European level guidance across sectors, as these SMEs experience shared problems between members states.

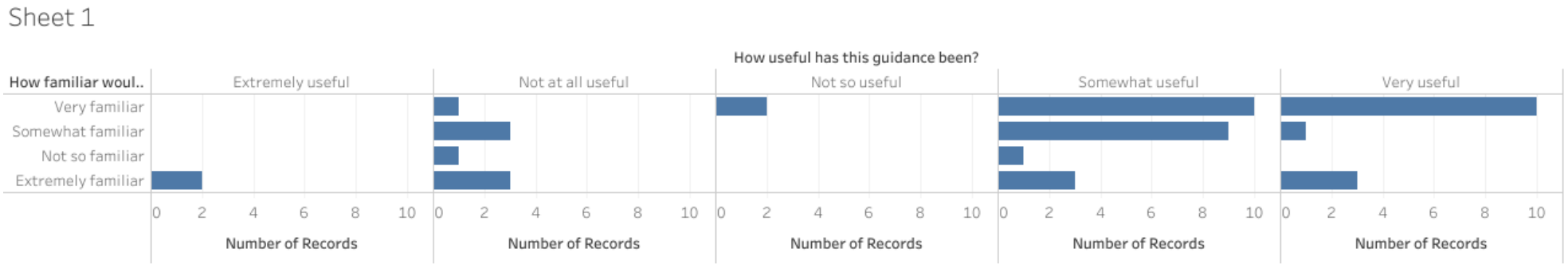

Figure 9a: Familiarity with the GDPR against usefulness of available guidance

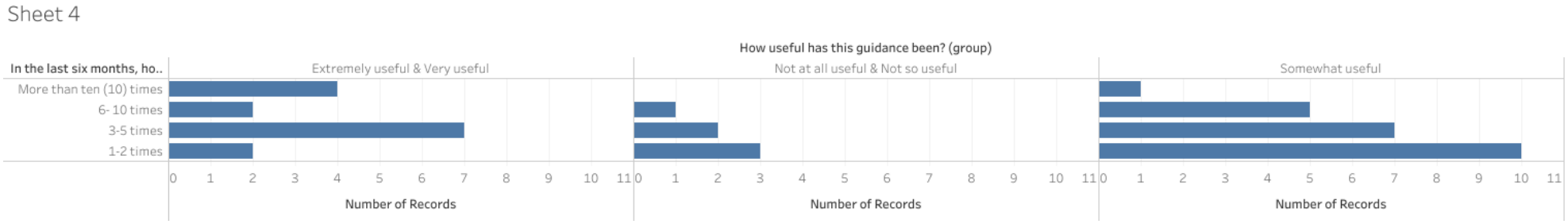

Figure 7: Frequency of accessing guidance against usefulness

Unsurprisingly, the people that find the guidance extremely or very useful are accessing it the most frequently, and those who find it not at all useful are accessing it much less frequently (see Figure 10). The distribution for "somewhat useful" is about what would be expected – a smaller number of more frequent uses and a larger number of occasional access. The distribution of "not useful" or "not very useful" is a similar shape (although with smaller numbers), suggesting that there are some SMEs who have to access it with some regularity who are not satisfied with it. The oddity in the useful/very useful category are again, those SMEs who access DPA guidance very frequently.

6.5. What training and guidance on the GDPR do SME associations provide?

We asked the SME associations if they offered any training or guidance on the GDPR. The responses divide into four categories.

Half of the interviewed SME associations have created some guidance and offer some training on the GDPR. The most common form for association provided guidance and training is support for GDPR-related queries in the provision of general legal advice and support. These organisations will respond to GDPR queries from the membership. These associations have also generated GDPR guidance documents and online resources, webinars, and have hosted workshops or conferences on the topics. These resources are generally not public and are provided just to members of the association.

Of these guidance and training providers, just under a quarter of the interviewed associations have created and offer a very substantial amount of training and guidance on the GDPR. These additional activities have included: a privacy toolkit, an SME cybersecurity guide, codes of conduct for marketing and advertising, courses and workshops, templates (e.g. data processing agreements, privacy notice, consent agreement etc), hosting a network for compliance professionals (not just data protection but also ethics), integrating GDPR compliance into broader compliance training, courses offering GDPR certification.

The remaining half of associations did not currently offer any GDPR guidance or training. Of these, four associations told us that they had previously created and offered GDPR training but no longer believed that this was something they could provide to their membership. Reasons given for this suspension in training was lack of demand and an unwillingness to pay for such training, as well as other sources of guidance being available (for example, they would direct queries they received to the national DPA website), and not yet having the resources to update pre-GDPR toolkits. There had been an identified demand for GDPR guidance prior to the May 2018 but this was perceived by the relevant association as having dissipated.

6.5.1. Where are SME associations finding guidance?

We asked the interview participants if they had identified any useful sources of guidance for SMEs on data protection which they were recommending to their membership. By far the most common source mentioned was **national supervisory authorities** / DPAs. A secondary source for several associations were the **DPAs of other EU member states** (explicitly mentioned by name were UK, Ireland, France, Poland). In most of these cases, a shared language is a key factor in this. The associations and their members would look for resources from other DPAs where there is a shared language (e.g. UK, IE or France/French speakers in BE). The UK's Information Commissioner's Office (ICO) was mentioned several times by pan-EU associations as a source of practical, usable guidance appropriate for SMEs.[8] Representatives from pan-EU and international organisations were able to identify guidance from multiple EU DPAs. Other identified sources of guidance included **ICT organisations**, **data protection networks**, **sectoral associations**, and other national organisations. Some respondents identified free guidance material available from **law firms**, for example, blog articles on their websites or downloadable whitepapers. However, others expressed concern about recommending guidance not produced by the regulators, including privately produced tools, as these are effectively untested and seen as risky to rely upon. Several respondents stated that they did not use external guidance material and had produced their own for their membership. It was suggested that association members were very likely to finding their own guidance from multiple sources using simple **web searches**, but that the associations themselves were not advocating this.

[8] This might however be a bias from our interviews being primarily conducted in English. Interviews conducted in other languages with participants with different fluencies could have produced different outcomes. The ICO's guidance could however become a lost resource, or worse a source of inappropriate guidance if there is too much divergence between EU and UK data protection regimes in the event of Brexit.

7. Key Challenges for SMEs

7.1. Key GDPR challenges for SME association members

From the SME association interviews, we can identify the following key GDPR challenges for SMEs (as understood by the SME association representatives):

- The costs of compliance – both in terms of money and time spent by personnel.
    - Minimum compliance is challenging for small organisations and those with limited infrastructure.
    - Some companies do not have the resources to do GDPR compliance. For those that do, it is an additional financial burden. For some it is reported as being overwhelming.
    - Cost of training new staff can also be high and taking GDPR awareness beyond the management level.
    - The (potential) costs of having a DPO.
    - Time to implement.
- SMEs lack internal data protection expertise and costs for external consulting are prohibitively high.
    - Lack of trust in lawyers and consultants in the field (yet also a reliance upon these as one of the main ways of getting to compliance).
    - Consultants focused on extremely risk-averse or conservative approach to compliance, requiring too much effort from SMEs.
- Costs/challenge of reviewing existing and established practices. Changing daily routines and business practices to comply with the GDPR, including organisational cultures and the way that people are used to working. Adapting to follow the legal rules.
    - E.g. website privacy policies and privacy notices
    - E.g. Use of data from customer loyalty cards for various business purposes.
    - Can they continue to use their existing customer contacts and mailing lists for marketing purposes (often containing both clients and potential clients)? Particularly important for SMEs because of their reliance upon repeat business.
    - Dealing with the large amount of GDPR information
    - GDPR cuts across many different areas of their business
- Fear and fear-related uncertainly / over-caution
    - of being fined
    - of complaints
    - of doing communication and marketing
- Misinformation about GDPR requirements.

- A lack of practical, applicable guidance on:
    - How the GDPR is interpreted and applied in practice
    - Fundamentals – e.g. assessing what data is necessary for a given purpose and what is not, examples of personal data,
    - Translating the GDPR into non-legal language, particularly connecting to business values (e.g. connect the GDPR to the values of an SME – that it is small, family run etc.
    - Data limitation for organisations doing a very wide range of activities (multiple purposes)
    - Specific activities
        - Gap analysis
        - Training
        - Data retention
        - Passing CCTV footage to law enforcement
        - Creating and maintaining documentation for compliance
        - The use of website tracking cookies
        - Data subject access requests and verifying identities.
        - Processing employee data (and correct legal basis).
    - Best practices and strategies
        - E.g. how best to get consent without making the process burdensome, bureaucratic and inefficient.
        - What should be in a data protection policy
        - Available technologies (e.g. for security or data management)
        - Processes
        - Data inventories
        - Contracts with service providers
        - Handling data subject rights, including rights to erasure
- A lack of clarity around
    - Where to start amongst the apparent complexity of all the GDPR requirements
    - Transfers of data to third countries (SMEs don't have to be big to be involved in cross-border trade)
    - Lawful basis for processing – particularly legitimate interest
    - Controller/processor relationships
    - One-stop shop and cross-national consistency
    - Data portability
    - Role of the EDPB
    - Open-ended concepts, such as large-scale data processing
    - Distinguishing between GDPR, privacy and e-privacy regimes

    - What exactly other companies are being fined for, and what they have done wrong (so that this can be avoided)
    - The positive business case for the GDPR
    - Concepts such as accountability, fairness, minimisation, confidentiality and data hygiene
- Conservative application of the GDPR by DPAs[9]
- The change of mindset required for risk-based rather than formal processes within the GDPR – e.g. accountability and for data protection-by-design.
- Issues with the nature of the GDPR itself in terms of:
    - Large, "heavy", complex document
    - No real opt-outs, or exceptions for SMEs
    - Difficult to comply in everyday scenarios – e.g. receiving a business card.
    - Perceived lack of cohesion across the EU

7.2. Key GDPR challenges for SMEs

We asked the survey respondents and interview participants[10] what (if any) had been their biggest challenges arising from the GDPR? Common challenges included:

- The time commitment needed to get ready for the GDPR
    - Also experience of time pressure up to May 2018
    - Having no additional resources to prepare
- Becoming familiar with the (new) rules and regulations / Trying to get an overview of what is required.
    - Vague, non-specific terminology
    - Legal terminology
    - Complicated for non-experts
    - Adding GDPR requirements to all the other requirements on a newly started business.
    - Required changes across all areas of work
- **Understanding what changes need to be made** to be compliant
    - Understanding what documentation is required.
    - Deciding what data can be kept and what must be deleted – deletion and retention policies
    - Deciding on proper level of implementation / what counts as "good enough"?
    - Data minimisation
    - Technical and organisational measures

[9] FEDMA, 'FEDMA position paper on transparency under article 14 of the GDPR' (9 May 2019).
[10] The survey had a larger number of key challenges identified, which is expected given the higher number of participants, but the broad types of challenges identified were similar.

- Implementation of changes
    - Changes in IT systems
    - **Developing and describing new procedures and processes**
    - Integrating GDPR processes with daily workflow and business processes.
    - Setting up processes for manual handling of physical copies of personal data.
    - Coherence between theory / legal and operational/practical aspects
    - Getting the company to prioritise these changes
    - CV/HR data handling
- **Getting staff to understanding the importance of data protection** and doing appropriate staff training.
- Documentation
    - New data protection policy
    - Producing appropriate documentation / records
    - Properly documenting and evidencing lawfulness of processing
    - properly documenting relationships with third parties (e.g. controller/processor).
    - Providing and accrediting compliance
- Third party relationships
    - Making arrangements with both customers and suppliers
    - Determining processor/controller relationships.
    - Power inequalities between processors and controllers when making agreements
    - Establishing legal consequences with third parties
    - Getting customers to understand new practices (e.g. new consent forms).
- Finding straightforward and appropriate guidance
    - Avoiding GDPR “fake news”
    - Lack of expert consensus - Experts having differences of opinion
    - Hiring experts too expensive for small business
- Practical challenges
    - Data anonymisation
    - Implementation of opt-in/out features.
    - Following up and maintaining organisational and technical measures post GDPR implementation.
    - Information security / securing against hacking
- Data protection incidents
- Understanding and making use of appropriate cryptography (e.g. for emails).
- A more conservative business environment
- That the requirements are the same for small and large businesses.

The challenges in bold were the most commonly mentioned challenges for SMEs: Understanding what needed to be done, then developing new processes and getting staff to understand why these changes were necessary and important.

> *"We spent a huge amount of time trying to get familiar with the rules and regulation and seeking guidance in how to act, what changes to implement to ensure all the requirements are met." – Tourism and Entertainment SME, Denmark.*

7.3. Myths believed by SMEs

From our interviews with SME associations, we were able to identify general myths and assumptions that SMEs may hold that may interfere with their data protection activity. Such myths include the following:

- That data protection / the GDPR doesn't apply to them
  - Not thinking of what they hold/process as "data"
- That they will not be investigated or fined
  - Big fines are for big companies
- That you always need consent of the data subject to process personal data
- They are not handling sensitive data because they're not in the health industry
- That the GDPR is a settled issue and this is all a done thing.
  - "The GDPR" was a one-time thing
- GDPR compliance as a tick-box exercise, not a process.
- That "data protection" is about one singular issue (e.g. CCTV, data access requests) and nothing else.

7.4. Issues for SME associations

Our questions to SME associations were focused upon the experiences and perspectives of their members. However, in this process some of the associations also told us about challenges they faced as umbrella organisations when engaged in the policy field of personal data protection at the EU level and when attempting to represent the interests and perspectives of their members on the GDPR. Some associations expressed concern that EC stakeholder groups on data protection tend to be dominated by representatives of larger industry, to the exclusion of SME representatives. Two EU-wide associations expressed concern about the consistency of implementation of the GDPR across Member States. They highlighted the need for closer cooperation with DPAs on this level of detail, but also in those areas where there is national flexibility or specific national implementations. Whilst

formal broader statements from DPAs (which come closer to the legal text) are more consistent, there is a greater level of inconsistency within practical examples (which are the type of guidance that SMEs are expressing a need for). Finally, an SME association from outside the EU reflected that SMEs outside the EU are very concerned to process data in line with the GDPR and are concerned about enforcement against them.

8. How can data protection authorities support SME associations and their membership?

STAR II is particularly interested in the actions that data protection authorities can take to support SMEs in data protection. This is important for raising best practices and for determining what additional supporting activity can be undertaken by a project such as ours. To this end, we asked several questions in the survey and the interviews regarding the positive steps that DPAs could take from an SME perspective.

We asked SME survey respondents what their data protection authority could do that would help the SME comply with the GDPR. "How-to" and "clear" were the most common terms that emerged from these responses. The two most requested actions were:

- Create more guidance, in simple and clear layman's terms, for commonly encountered data protection situations.
    - There was also support for specific sectoral guides.
- Provide practical advice, that is specific about how to act in everyday data protection situations.
    - This guidance must be specific
    - This advice should contain practical examples, either real-life or fictional

There was a clearly expressed demand to learn from **real-life practical examples** (e.g. What are other people doing? What would this look like in practice? What does this mean for a business like mine?) and to have clear, step-by-step guides that set out exactly what they should do be become compliant. Several SMEs wanted their DPA to provide **quicker answers to questions** and give answers that related to the specifics of the question, with similar qualities to those given for guidance above. There were also many single-instance suggestions including:

- Creating standards for small companies
- Evaluate experiences from enforcement actions and cases and report this back to SMEs
- Create and maintain an SME newsletter
- Run training courses for SMEs
- Produce sample data protection policy
- Review and reconcile GDPR implementation on a regular basis.[11]
- Increase DPA visibility

[11] Arguably, this is the role of the GDPR consistency mechanism and the EDPB.

- Evaluate our compliance effort and tell us how we are doing, and
- "not meddle with our business"

We asked the SME association representatives how EU data protection authorities could help SME associations and their membership. They provided the following requests:

- Provide more interpretation of the GDPR and its obligations upon SMEs
  Provide concrete and specific examples surrounding typical scenarios such as when a DPO is required
- Provide more guidance, including "how-to guides" on:
  - Information security
  - Marketing / communication activities
    - Particularly email marketing
  - HR matters
    - Recruitment / employment
  - Legitimate interests
  - Commercial activities
  - Data processing records
  - How to run a customer database
  - Retention schemes and when to delete data
  - Anonymisation
    - Including anonymisation of physical records
- Provide specific guidance for SMEs
- Provide specific guidance for specialists and generalists in important topic areas (e.g. marketing for direct marking companies, and marketing for general SMEs)
- Provide templates
  - Records of processing (Article 30)
  - Inventory / Data audit
  - Consent forms
- Greater engagement with trade associations
  - Participate in events organised by the association for their membership
- Showcase / present best practices in data protection from other countries
- Provide e-learning materials.
- Understand that as a regulator, the supervisory authorities can be seen as threatening to SMEs - Adopt an approach that reduces this fear.
- Create/provide tools that allow for self-assessment (to help SMEs understand what situation they are in, and which provisions apply to them).

It was suggested that GDPR guidance should focus upon the vulnerabilities of SMEs, especially in information security and IT risks (dealing with a cyber attacking, managing databases appropriately, risk assessments, gap analyses).

In terms of the format of materials, visual material which is short and in everyday language was recommended. E-learning material and webinars focused upon specific challenges were also mentioned as being attractive by several respondents.

One association respondent did tell us that it is too late for the DPAs to provide guidance for SMEs (linked to the belief that the GDPR is over and done with). Another told us that they believed they had provided the guidance that their members required. In the survey, a small number of respondents suggest that it was currently too late for the data protection authorities to produce guidance.

8.1. Questions that SMEs want answering (by DPAs?)

We asked the associations what key questions they believe their members wanted answering. They told us, that their members wanted answer to the following questions:

- How should SMEs respond to a cyber-attack?
    - How can we mitigate fines when a hack is a result of a state-level action?
- When is a DPO required?
    - What makes a suitable DPO?
    - Should we recruit or appoint a DPO?
- What are appropriate data retention periods?
    - How should we evaluate how long we should hold data for?
- When should we share data with the police – what is required?
- Is it ok to use services from Google, Facebook, Amazon, etc? given that we cannot negotiate services with these large organisations, can't really visit their premises, and can't independently verify their data handling practices. However, these services are important enablers for small business.
- What kind of encryption is enough to say that stored personal data is safe?
- What is high risk data processing?
- When is a data protection impact assessment required?
- What counts as a legitimate interest for an SME?
- How should we handle ordinary, everyday contact information – e.g. business cards?

From the face-to-face interviews the following questions emerged:

- Will there be inspections? When and how will these take place?
- Is there any difference between how the GDPR is applied to small and large business?
- What are the risks of non-compliance?
- How should I manage requests and legal claims by data subjects?
- What tools and guidance has (the national DPA) provided for SMEs?
- What channels is the national DPA using to communicate with companies like mine?
- How "mature" are we in our GDPR compliance activity? / are we doing this right?

8.1.1. Challenging compliance issues around the data protection principles for SMEs

We asked the SME associations whether any data protection principles were especially challenging. Respondents were divided upon the importance of data protection principles. Some felt that particular principles needed further explanation, definition or guidance. A second group felt that all data protection principles would benefit from further guidance, including around explaining why particular principles were important (which the GDPR itself does not do). A third group suggested that principles was the wrong focus for SMEs, who would not pay attention to guidance at this level of abstraction. Within this group, there were respondents who criticised the principles-based data protection model, in which data protection is an active process where adherence to these principles needs to be continuously considered and a large amount of interpretation needs to be done, as inappropriate for SMEs. In terms of the principles which SME associations expressed as challenging and in need of more guidance, these were:

- All of them (x2)
- Lawfulness of processing – legitimate interest
- Lawfulness of processing - Consent –(It was suggested that a distinction between contractual law and consent challenges the "free business model")
- Data retention – comparison with existing practices (e.g. retaining CVs) or with data used to enrich other activities.
- Data limitation – particularly when there are a large range of activities.

In addition, although it is recognised that these do not constitute data protection principles, the following issues were also mentioned:

- Definition and meaning of personal data
- Data security – what counts as appropriate security measures

8.2. What guidance do SMEs want?

The survey asked respondents which areas of the GDPR would they like to have more guidance on. They could select multiple areas if they wished to (see Figure 11).

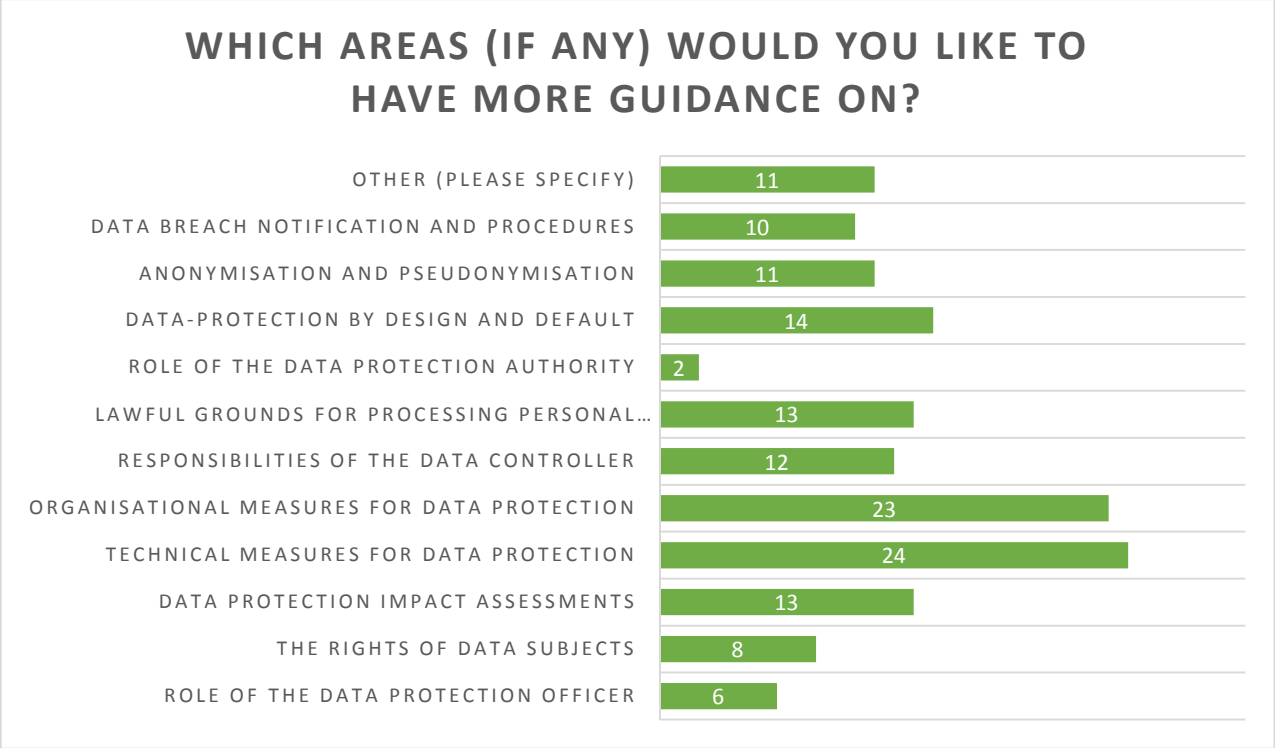

Figure 11: Areas on which SMEs desire more guidance

The clear message from this is that whilst guidance is sought across the range of key GDPR areas and that there is little appetite for an explanation of the role of the data protection authorities.[12] There is however lots of demand from SMEs for guidance on technical and organisational measures for data protection.

Responses to this survey question suggest that SMEs would appreciate concrete guidance across the areas of the GDPR which stipulate that data controllers and processors are required to adopt "appropriate technical and organisational measures". These include for example, technical and organisational measures: to ensure that the requirements of the regulation are met (Recital 78); to ensure that factors that result in inaccuracies in personal data are corrected (Recital 71); for data minimisation (Recital 156); to safeguard the rights

[12] In contrast, the STAR project study of existing GDPR training materials and approaches found that the EU data protection authorities themselves considered explaining their role a very important part of the training material they produced and something they wanted to see present in training material developed by third parties. Available at: https://projectstareu.files.wordpress.com/2018/06/star-d2-2-report-on-the-findings-of-the-interviews-v1-1-final.pdf

and freedoms of the data subject (Article 5(1)f); and to ensure and be able to demonstrate that processing is performed in accordance with the Regulation (Article 24(1)).

There was also quite a strong demand for guidance on data protection by design and default and data protection impact assessments. Responses in the 'other' category included:

- Data processor agreements
- Data controller and processor responsibilities (x3)
- Staff training and getting staff to understand the importance
- Better templates
- Impacts on data transfer to USA and UK (post-Brexit).

From the face to face interviews, more guidance was requested on:

- All data protection principles
- All data subject rights
- Implementing data minimisation in practice
- Implementing data accuracy in practice
- Transparency
- Data retention
- Right of Erasure (particularly in relation to CCTV)
- The right to portability

8.2.1. Specific concerns - Direct marketing

SME associations and SMEs were asked a specific question about any concerns or considerations around direct marketing. Multiple SME associations reported a negative impact on business activities in the field of direct marketing due to the GDPR. The use of direct marketing (for example advertising emails and newsletters) was seen as quite common among and important for SMEs. They told us that direct marketing has been reduced due to fear about potential fines. The Associations reported that many companies have been unable to get consent from their existing (pre-25 May 2018) databases and that this has been causing problems for their marketing effort – presumably as they are unwilling to use those databases. Some members have started from scratch with their newsletters, in order to make sure that they consent.

One respondent informed us that the combination of the GDPR, cookie law, the e-Privacy draft, e-commerce law and e-marking laws was too burdensome and was effectively killing the direct marketing industry.

Other associations discussed concerns around how best to reconcile or align GDPR compliance with e-Privacy compliance (especially given the in-progress status of that legislative reform). They were worried about recommending one set of practices to comply with the GDPR that would then have to be adjusted with the e-Privacy regulation (expressing the view that e-Privacy regime did not include a consideration of legitimate interests). It was however noted that for organisations that already had consent for direct marketing, they would not have to adopt a radically different approach to comply with the GDPR. Therefore, companies raising issues about consent for direct marking under the GDPR regime may simply not have had consent for the direct marketing and associated processing of personal contact information they were previously performing. A related concern was that demanding too much from consent (in contrast with legitimate interest) risks creating a burdensome and alienating experience for the customers of SMEs (presumably if they received poorly executed or legalese consent requests before they see anything attractive or interesting from the SME). Aligning GDPR compliance and adherence with Directive 2009/136/EC[13] was also raised as an issue.

Direct marketing was an area where many associations had received queries from their membership. Many associations suggested their members would welcome clear, practical guidance on how to run direct marketing activities in a way that is compliant with the GDPR requirements – in particular, making customer databases, sending direct marketing emails, and making and acquiring new business contacts.

The SMEs we interviewed did not largely see direct marketing as a problem. Either they considered they were not doing direct marketing (although in some cases, they may have been), or their communications were business to business. Some had implemented new approaches for direct marketing, for example, one SME told us they had dropped a contact list used for text messages about sales from around 2000 contacts to 800 where they know they have consent, whilst another described that this was an area where they were particularly careful. The small number in the sample that did regularly conduct direct marketing activities felt that they were aware of and meeting the GDPR requirements.

[13] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services. Also relevant are Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance).

8.2.2. Specific concerns – employment

We also asked the SME associations and SMEs about the specific concerns they have concerning data protection and employment. Employment was seen as a heavily regulated area that required specific attention but that also had a high level of national variation in legal requirements, which applies to SMEs with employees in more than one country. Most employment related data processing was seen as being conducted under the performance of a contractual relationship. The GDPR had increased some of the obligations around informing employees about how their data was being processed and is seen as having created new requirements to 1) provide detailed information and 2) gain formal consent before using photos. Some associations sought greater clarity on the data protection provisions that should typically be included in an employment contract and how best to provide information on data processes to employees. A concern was raised that the lack of harmonisation between EU countries around whether processing of employee data could be considered under consent as a legal ground.

General challenges mentioned in this area included: using pictures of employees for marketing (e.g. using employees in photos, using photos to promote events); access to employee data from third parties; retention of data on former employees; managing next-of-kin and emergency contact details; monitoring by employers of staff social media or email use (including during lunch breaks); and data processing of employees not related to the core of their job, or explicit job roles in their contracts.

The face-to-face SME interviews identified some SMEs who had not been thinking about the GDPR in an employment context (only thinking about customer data). For others they felt that staff details and info was handled by their accountant. For a micro-SME this wasn't an issue because the business was run and staffed by the owner.

8.3. Capturing SMEs attention on GDPR issues

We asked SME associations what they thought was the most effective way to get their members to pay attention to compliance-related topics such as the GDPR. This has not only implications for projects such as STAR II but could also advise the communication activities of DPAs. They suggested the following strategies:

- Providing members with information on the fines under the GDPR – effectively highlighting the potential cost of non-compliance. This was linked to the need for DPAS to undertake enforcement action. Similarly, making use of high-profile data breaches and enforcement cases as a vector to promote awareness of the GDPR

requirements. Associations suggested that a breach by an SME, followed by a fine, would capture the attention of other SMEs.

- Keeping the topic at the forefront of mind through regular communication, for example, the inclusion of data protection related matters in weekly newsletter and on website articles, making use of their mailing lists of members.
- Undertaking visible projects – for example, participating in a consultation exercise with a ministry.
- Showcasing best practices (including from competitors and rivals).
- Providing case studies.
- Organisation of events and workshops at national level
- Social media was identified as a potential tool for this but heavily reliant upon the topics. LinkedIn was identified as particularly valuable for one association as most of its membership were users.
- Physical roadshows and trade fair booths.
- Using expert groups (e.g. IAPP) as channels to reach SMEs.

(Unsurprisingly), several SME and industry associations suggested that being a member of an association was one of the most effective ways for an SME to become and remain informed about GDPR-related issues, requirements and best practices concerning compliance with other relevant laws. They identified their own guidance, their research work, working groups and communication channels (newsletters, social media, events, trade fairs etc) as effective ways to reach SMEs. Several expressed some concern about those companies that were not members. Some were however cautious about their ability to give legal advice to SMEs, due to a risk of liability.

It was suggested that the peak of attention for the GDPR was at the time of it coming into force in May 2018, and that this attention, and associated sense of urgency to act, is now reducing from this peak.

9. STAR II Tools and support

9.1. A data protection helpline/hot-desk for SMEs

We asked representatives from the SME associations, and the face-to-face interview participants their opinion on the usefulness of a hotline or helpdesk service offered by DPAs in coordination with other data protection experts from SMEs and academia. This activity comprises part of the STAR II project and is being run by NAIH (see future deliverables D3.1., D3.2. and D3.3.)

About a third of SME associations simply thought that this would be a useful contribution. ("it would be amazing", "important", "help with dialogue").A small number disagreed completely. One association reported providing a commercial law helpline and an employment law helpline which can both cover GDPR-related queries for their members. Another respondent raised cultural questions around hotlines, relating them to more general tendencies around asking for help and the risk of appearing unknowledgeable. In the face-to-face interviews, the large majority expressed an interest in the hotline, with the small minority of participants straightforwardly telling us they wouldn't use it as they didn't really process much personal data.

The majority of SME associations interviewed thought a helpline could be useful, but offered various caveats and suggestions for how its benefit might be maximised. They suggested that a helpline would be useful if it provided practical advice and support and was able to give quick (with at maximum a one-week response time), specific answers to questions. It was suggested that a helpline would require extensive marketing because SMEs are hard to reach, and funds dedicated to that. Several noted that it would be advantageous if the helpline produced written guidance and would be fantastic if the advice was binding (but they were not anticipating this). In the face-to-face interviews, caveats included that the hotline be staffed by experts, and would ideally be cost-free.

Respondents identified existing hotlines operated by DPAs (Denmark, Spain, Latvia, Ireland) and hotlines overall as a relatively common practice– some of which have adequate response times (faster for phone than email), whilst others were seen as quite slow. There are some challenges with the knowledge level of existing employees. Association representatives suggested that the demand for law firms for GDPR experts was acting as a drain upon DPAs. One association reported on feedback from their members that they did not find the DPA phone service too helpful. Their reported problems were that the advice received was too complex, and that the DPA did not consider the advice given on this helpline to be legal opinion.

There was disagreement about the appropriate institutional home for such a helpline. Several respondents suggested that the helpline would need to be established by the DPA to be trusted and to be authoritative (and therefore worth using for SMEs). One interviewee suggested that DPAs should have a specialist department for assisting business and helping companies comply with the GDPR. However, others expressed concern with hotlines run directly by national DPAs, mainly because of the dual role of supervisory authorities as both source of guidance and best practice, but also as regulator and enforcer. They suggested that their lack of clarity as to the role of the DPA – is it for citizens or for SMEs – essentially, does asking a question increases the chances of complying or does it raise the risk of enforcement? One reported that SME association members would be more likely to come to the associations for help, again because of a perception of lower risk. It was considered that companies could get into trouble if they spoke to the regulator. There was some support for a specifically pan-European hotline -especially useful for companies that operated across different Member States. There was support for a helpdesk located within the EDPB.

There was a further lack of consensus about the preferred modality for a hotline – email was preferred by some because it created a written record of what was discussed and what was advised by the DPA. They reported generally receiving queries from their members by email, and SMEs being comfortable with this mode of communication. Whilst phone calls were preferred by others because of the speed of response – getting an answer, even if imperfect at the time when it is needed, rather than waiting for a written response – and in one case, because of the potential for anonymity, exposing the company to less risk. A phone call was also seen as allowing for a better explanation of a problem, and for a quicker back-and-forth interaction when there is a confusion or lack of clarity. The SME interviews reflected two types of time pressure on SMEs. The first pressure was the time available to create and ask a question – for these SMEs an email is preferable because it is quick to write. The second time pressure is the time it takes to get a response, for these SMEs the phone allows for a quicker response, even if they have to spend some time waiting on the phone.

It was suggested that instead of a helpline, perhaps raising awareness of the existing tools would be more useful – there is guidance there, but it is not being used. This would reduce the number of times that SMEs would need to ask questions – the answers are likely in the existing guidance for most cases.

In terms of language and national origin of the hotline, there was a definite demand for hotlines operated in local languages and sensitive to local legal particularities. it was noted that SMEs need support in their national languages, particularly given the technical nature

of the topics being discussed, and the need for precision. A phone service would have a greater need for linguistic fluency than a written service.

They could make use of a hotline provided by another member states' DPA but would likely have a strong preference for getting support from their own national regulator. An additional hotline would need something special to make it stand out from existing offerings. It was suggested by one respondent that if a helpline were staffed by sufficiently talented and knowledgeable people, then this would be an attraction to make use of as an additional service. In the face-to-face interviews we explicitly asked if people's opinion of a helpline would change if it was offered by a DPA other than their national one. For many respondents, they did not feel this was too important, but that it being offered by their national DPA did increase confidence. However, for a significant minority it was vital that the support be offered in their national language and by their national DPA. One respondent explained that the DPA providing it did not matter provided "the advice is consistent, it applies in [home country] and is appropriate to company size". Several associations remarked that local DPAs should be involved in running the service, or at the very least be prepared to endorse it and its guidance. Feeding into these concerns furthermore were the potential national differences in the application of the GDPR and also other national legislative differences that interact with the domain of the GDPR. It was considered that these would need local advice and expertise for accurate understanding and advice. International SME associations reported that they did consider that there were different interpretations of the GDPR in different national guidance they had observed, and this would create troubling implications for any cross-border hotline.

9.2. A GDPR Handbook for SMEs

One of the supporting activities envisaged for the STAR II project is the production of a GDPR handbook targeted at EU SMEs, with the intention of supporting them on key topics of interest and otherwise facilitating their achievement of GDPR compliance. We asked the SME association representatives and SMEs we interviewed for their perspective on this, and what it should contain.

9.2.1. Style and approach

- Practical - The most common request, was that the handbook be practical. It should be possible for an SME to follow the steps and advice contained in the handbook.
- It should make heavy use of examples and case studies – particularly to clarify GDPR obligations. One respondent even suggested one initial page of explanation and then making a handbook that consisted solely of case study examples for each of the key areas of the GDPR. Another suggested working up an example using a "standard

company model – a company constituted and acting in a very common manner for the SME sector, with no particular data processing oddities. SMEs using the guide could compare themselves to this, and if they were a "standard" company, then they could simply enact the steps in the guide.
    - Case studies should include success stories, and how compliance was implemented, rather than just raising challenges and problems.
    - Real life case studies were preferred to artificial/created case studies.
    - Walked-through scenarios – explaining the steps and reasons at each decision
- Provide steps for compliance
- Easily understandable – It should be written avoiding jargon and explain terms. It should be accessible, understanding the wide range of backgrounds involved in SMEs.
    - A layered approach was suggested – starting with a description of formal requirements, followed by further guidance for businesses with time and resources.
    - It should be brief, not a huge document that must be trawled through
- Provide templates (useful for increasing consistency, and getting SMEs doing the right thing quickly) and tools. Standard documents should be included.
    - Privacy notice template
    - Data protection template
- Myth busting – devoting some space in the handbook to countering common myths and mistaken beliefs (see section 7.3for further detail on the myths that SME associations believe their members hold about the GDPR).
- Include a Frequently Asked Question section.
    - Again, with examples
- A digital version was generally preferred (including by almost all the SMEs interviewed directly), however some associations have been asked by their members for print copies of their guidance, so there is demand for both formats.
    - Digital version could allow for printable, searchable and copy-paste functions.
    - An interactive online version that could output completed templates was requested. This was compared to the "Facilita" tool, developed by the AEPD (the Spanish DPA).[14] The ability to answer questions to establish a required level of action to take was also requested in this context.
- Not too many external links.

[14] https://www.aepd.es/herramientas/facilita.html

9.2.2. Contents and topics

Guidance on the following topics would be appreciated[15]:

- Direct marketing
- IT environment for data protection
    - Validity of software certification
- Data security measures
    - Passwords
    - Encryption
- The concept of risk (and understanding data protection as an ongoing risk management activity, not a one-time event).
    - Including examples of data protection risks – what can go wrong
- Explain the role of SMEs in the digital single market
- Advice tailored to ICT, retail and cloud computing
    - SME data processing using third party applications and services (e.g. Google, Apple, Facebook).
- Need to appoint a DPO
- Summary of national differences in GDPR implementation and the potential impacts of these on SMEs.
- How to conduct the various self-assessment and risk-assessment activities required by the GDPR
    - E.g. when data is no longer necessary for original purpose and should be deleted
    - DPIA
- How to write standard documentation
- Details on where to go to get further information (DPAs, Associations, training providers, etc).
    - List of useful phone numbers

Concerns and risks that were identified included:

- There are already handbooks in circulation – respondents identified an IAPP handbook[16], a Fundamental Rights Agency handbook[17] and an EC guidance website[18].

[15] See also the topics addressed in the key GDPR issues and questions sections of this report, Sections 7 and 8.
[16] https://iapp.org/resources/article/handbook-on-european-data-protection-law/
[17] https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law
[18] https://ec.europa.eu/justice/smedataprotect/index_en.htm

- There was some expression of concern about the added value of a one more handbook on the GDPR. Two representatives told us that they would prefer to see something that was more specific to types of business, given then the variation in needs across the SME sector.
- There was concern about language, with several requests for the handbook to be available in (multiple) national languages to be accessible for the majority of SMEs.
- Several respondents suggested that short video clips would be more suitable than a handbook. In the SME interviews, it was suggested that an interactive website, e-learning module, and regular, updated seminars would be preferable to a handbook.
- One SME we interviewed suggested that a handbook was problematic as they just did not have time to read it.

10. Moving Forward with STAR II: Towards developing guidance on good practice in DPA awareness raising with SMEs and a handbook for SMEs

10.1. Core Messages for the Handbook

At the end of the questionnaires/interviews, respondents were asked about the core questions that should be addressed with the STAR II handbook for SMEs. Many DPAs pointed to the array of issues already raised in section 6.3.2. of Deliverable D2.1 and which appear to be broadly covered in the SME specific guidance documents which a few DPAs have already developed. In this report, SME challenges are largely covered in Section 7 and helpful responses for the handbook in Section 9.2. If STAR II wants to maximise the benefit of the handbook, it is useful to explore how best to meet these needs and complement existing resources. This section attempts to draw out ideas primarily identified by the SMEs and SME associations, or that logically follow on from the information they provided.

In moving forward with the handbook for SMEs, STAR II should consider the following suggestions:

1. **A generic SME handbook focused predominantly on a compilation of examples and templates.** It was clear from the totality of information provided to the STAR II project that SMEs benefit from concrete examples. Such a strategy could be used to bolster the handbooks already in existence and be translated by DPAs into relevant languages. Borrowing on the strategies/tools employed by larger organisations could help here. (These examples may first need to be endorsed by a range of DPAs.)
2. **A sector specific handbook.** One DPA suggested that it would be of benefit for the handbook to be sector specific. For example, it could apply to online shops, photography businesses, hairdressers, owners of small hotels and hostels, nutrition advisers, human resources professionals, or CCTV businesses. The project would have to identify the appropriate level of granularity for appropriate sectors.
3. **A risk-focused handbook.** A core message coming through from the STAR II data is that SMEs face a methodological challenge with the GDPR in the sense that they may understand it conceptually but less so how it applies to their specific context. A handbook focused on how SMEs should conduct risk assessments and the technical and operational measures resulting from these assessments may be of special benefit.
4. **'Selling' the GDPR handbook.** This handbook might be ideologically driven, emphasising the key messages behind the GDPR which a compliant SME could market to their clients. This could include the messages of consumer trust, efficiency, sustainability and data security. It could also include strategies to demonstrate compliance to the public (and not just the DPA), for example, the

identification of a DPO, signing up to a sector Code of Conduct, or appointing a Personal Data Protection Champion. It could also include guidance on how to "sell" GDPR-driven changes and requirements to the staff of the SME.

5. **Myth-busting handbook.** This possibility emerged more concretely from Deliverable D2.2 but it could include the points identified by some DPAs that the GDPR need not always be difficult or burdensome.

10.2. Core Messages for the DPA Best Practices Guidance

In developing the DPA best practice guidance, STAR II may wish to take forward some of the suggestions below which have been derived from the report findings. These have been presented to mirror the focus of sections 6 – 8 of Deliverable D2.1.

Concerning the identification of SME needs, STAR II should consider whether the following are best practices:

- **Formally recording issues raised with DPAs by SMEs.** This would be especially important in the forum through which DPAs interface with SMEs the most - the hotline/helpdesk. It would also serve as necessary data for the monitoring and evaluation of SME awareness-raising strategies and the success of any knowledge-based resources.
- **Maintaining strong (informal and accessible) relationships with SME associations.** SME associations have an active audience with SMEs in a way that is difficult for other bodies to achieve. Some SME associations described knowing DPA staff by name and able to call them at any time with queries.
- **Asking and assisting SME associations in taking the lead on needs identification research activities.** The research recognises that while capacity in many DPAs has grown since the advent of the GDPR, resources remain under demand. SME associations might be better placed to undertake research on baseline SME needs which can be used as a platform for DPAs to focus on knowledge-orientated guidance, such as the development of examples.
- **Undertaking commissioned research at specific intervals to assess awareness of specific issues.** It is important to ensure that the same research questions are asked more than once to be able to assess the effectiveness of any awareness-raising measures taken or general shift in SME needs. As mentioned above, this could be done in coordination with SME associations to avoid duplication of effort and maximise resources. The emphasis here is again on follow-up and mapping change.

Concerning the provision of resources to SMEs, STAR II should consider whether the following are best practices:

- **Operating as conduits or facilitators between the compliance departments of large organisations and SMEs to aid the borrowing of compliance strategies.** The data suggests that there is little difference in the substantive needs of larger organisations and SMEs but that the larger organisations can address these needs largely in-house. DPAs occupy an important intermediary space with potential that they could maximise for SMEs.
- **Focusing on the compilation of examples and templates.** It might benefit the DPA to work with DPAs across the EU to agree and share examples where possible.
- **Developing guidance with an emphasis on the notion of *time* to reflect the ongoing and proactive nature of the GDPR obligations, even if this ongoing resource is small.**
- **Reviewing the guidance produced against an accessibility criterion developed for SMEs.** This could include the accessibility of the language, i.e. business words, the practicality of the content, i.e. examples, templates, follow-on contact points, as well as inclusion factors, such as hearing or eyesight disabilities.
- SMEs find it challenging to assess proportionality and data protection risks of their operations and would rather have clear steps to take to comply with requirements stemming from the GDPR. However, they consider that many of their practices are fairly standard. Could such **standard assessments be made by DPAs**, perhaps with assistance of sectoral organisations, with guidance on how these might differ?
- Offering **multiple channels for SMEs** to contact DPAs, and being able to respond on those channels.
- Understanding the extent to which SMEs need to be aware of their guidance before they can access it, and the amount of their communications activity that is devoted to "pushing out" guidance to potential recipients.
- Production of **specific resources for employers**, as this (alongside marketing) could cover a significant proportion of personal data processing done by SMEs.

Concerning awareness-raising activities, STAR II should consider whether the following are best practices:

- **Ensuring that all SME communications include a focus on the strategic and financial benefits of the GDPR for business.** It appears that there may be a missed opportunity to 'sell' the GDPR, both to SMEs and by SMEs. Whether the GDPR can be genuinely called simple for SMEs is unclear. By emphasising the benefits for SMEs in terms of their customer base, it may be possible to garner greater ongoing interest.

- **Developing separate strategies for awareness-raising among isolated SMEs and engaged SMEs (e.g. sector engagement, rural/urban, technology literate etc).** The STAR II project is aware that many SMEs have not engaged with their national DPA and that some will also operate largely apart from SME associations. Such SMEs need to be distinguished from 'connected' SMEs and SMEs that operate with a high level of technological capacity.
- **Prioritising opportunities for personal interaction with SME representatives and SME associations.**